

MULTICAST COMMUNICATION SYSTEM

BACKGROUND OF THE INVENTION

5 Field of the Invention

The present invention relates to a multicast communication system and specifically relates to a multicast communication system whereby data relating to a prescribed data distribution service is communicated by multicasting. Also, the present invention relates to a multicast data transmission device and multicast data receiving device.

Description of the Related Art

15 In the Internet or an intranet, the well-known technique of IP multicasting is available whereby the same data is distributed to a large number of clients (clients belonging to the multicast group). Such IP multicasting is suitable for distributing data (content) such as music or video on the Internet or an intranet. In future, as use of IP multicasting for contents distribution becomes common, it is anticipated that there will be a demand for the ability to levy data distribution service charges (reception charges) by imposing charges on clients.

25 In these circumstances, in order to levy charges appropriately, it will be necessary that, of clients belonging to an IP multicast group, clients that have

subscribed to the data distribution service will be able to
view and listen to the distributed data, but clients that
have not subscribed to the data distribution service,
although they will be able to receive the distributed data,
5 will not be able to view and listen to it.

To achieve this, it is vital that the data
distribution source should be able to definitively
ascertain whether or not a client is subscribed to the data
distribution service and an encryption technique for
10 ensuring that only subscribed clients can view or listen to
the distributed data is also vital.

Furthermore, since there will be a large number of
receiving parties, a quantity-based method of charging
appears desirable, in which charging is effected in
15 accordance with the quantity of data received.

However, a presupposition of the encryption technique
that is currently implemented on the Internet is that the
data sending party and receiving party are in a one-to-one
(unicast) relationship. No consideration has therefore
20 been given to IP multicasting with a large number of
receiving parties and the current situation in regard to IP
multicasting is that the data are distributed in
unencrypted form.

A conventionally employed quantity-based charging
25 system is the pay-per-view system that is employed in CS
broadcasts etc; however, in this system, charging is
effected in program units. Consequently, even if

viewing/listening is interrupted during the program, the charge for viewing the entire program is still applied. Strictly speaking, therefore, it cannot be said that charging is effected on the basis of the quantity of data
5 received.

When images or music are distributed on the Internet, a more finely graduated charging system than the current pay-per-view is therefore demanded, which can cope with participation/withdrawal of receiving parties in units
10 shorter than program units.

SUMMARY OF THE INVENTION

In view of the above, an object of the present
15 invention is to enable encryption and decryption to be appropriately performed in multicast communications.

A further object of the present invention is to make it possible to ascertain which clients, of clients belonging to a multicast group, are subscribed to a data
20 distribution service.

Yet a further object of the present invention is to perform quantity-based charging in suitable fashion.

In order to achieve the foregoing object, a multicast communication system according to a first aspect of the
25 present invention is a multicast communication system having a multicast server for transmitting data relating to a prescribed data distribution service by multicasting, and

group by multicasting; a key encryption unit for encrypting
said first encryption key by using a second encryption key;
and a key transmission unit for transmitting the first
encryption key encrypted by said key encryption unit by
5 unicasting to at least one of the clients belonging to said
multicast group, said at least one client subscribing to
said data distribution service.

A multicast data receiving device according to a first
aspect of the present invention for receiving data relating
10 to a prescribed data distribution service transmitted by
multicasting comprises: a key decryption unit for
decrypting a encrypted first encryption key obtained by
subscribing to said data distribution service; a data
reception unit for receiving said data encrypted by using
15 said first encryption; and a data decryption unit for
decrypting the encrypted data received by said data
reception unit, by using the first encryption key obtained
by decryption of said key decryption unit.

According to the first aspect of the present invention,
20 the multicast server (or multicast data transmitting
device) encrypts the first encryption key employed in
encryption of the data, by using the second encryption key
and transmits this by unicasting to at least one client (or
multicast data receiving device) subscribing to the data
25 distribution service. When the at least one client
receives the encrypted first encryption key transmitted by
unicasting, it decrypts this using a decryption key. Next,

the multicast server encrypts the data using the first encryption key and transmits it by multicasting to clients belonging to the multicast group. When the client receives the encrypted data, it decrypts this using the first
5 encryption key obtained by decryption of the decryption key.

According to the first aspect of the invention, data relating to the prescribed data distribution service is encrypted. Also, only at least one client subscribing to this service can decrypt the encrypted data and secrecy of
10 the data is guaranteed in respect of clients that are not subscribed to this service. Consequently, data encryption can be appropriately performed in multicast communication.

A multicast communication system according to a second aspect of the present invention is a multicast
15 communication system having a multicast server for transmitting data relating to a prescribed data distribution service by multicasting and a plurality of clients belonging to a multicast group and that receive said data, said multicast server comprising: a key updating
20 unit for updating a data encryption key for encrypting said data, at intervals of a prescribed updating timing, to a data encryption key that is valid after the updating timing, said data encryption key that is valid after the updating timing being in a relationship that is obtained by applying
25 an updating key corresponding to a data encryption key that is valid before the updating timing to the data encryption key that is valid before the updating timing; an updating

key holding unit for generating or holding in advance said
updating key; a data encryption unit for encrypting said
data using a data encryption key that is valid currently; a
data transmission unit for transmitting said data encrypted
5 by said data encryption unit to said plurality of clients
by multicasting; a key encryption unit for encrypting the
updating key corresponding to the data encryption key that
is valid after the updating timing, at intervals of said
updating timing, using the data encryption key that is
10 valid after the updating timing; and an updating key
transmission unit for transmitting the updating key
encrypted by said key encryption unit to at least one of
said plurality of clients by unicasting or multicasting at
intervals of said updating timing, said at least one client
15 subscribing to said data distribution service; and said at
least one client comprising: a data reception unit for
receiving the encrypted data transmitted by said data
transmission unit; a data decryption unit for decrypting
said encrypted data received by said data reception unit,
20 using a data decryption key that is valid currently that is
the same as said data encryption key that is valid
currently; an updating key reception unit for receiving the
encrypted updating key transmitted by said updating key
transmission unit; an updating key decryption unit for
25 decrypting the encrypted updating key received by said
updating key reception unit, using said data decrypting key
that is valid currently; and a data decryption key updating

unit for updating a data decryption key that is valid
before said updating timing to a data decryption key that
is valid after the updating timing, at intervals of the
updating timing, said data decryption key that is valid
5 after the updating timing being generated by applying an
updating key obtained by decryption using a data decryption
key that is valid before the updating time to said data
decryption key that is valid before the updating timing, a
data decryption key on subscribing to said data
10 distribution service being given from outside.

A multicast data transmission device according to a
second aspect of the present invention comprises: a key
updating unit for updating a data encryption key for
encrypting data relating to a prescribed data distribution
15 service, at intervals of a prescribed updating timing, to a
data encryption key that is valid after the updating timing,
said data encryption key that is valid after the updating
timing being in a relationship that is obtained by applying
an updating key corresponding to a data encryption key that
20 is valid before the updating timing to the data encryption
key that is valid before the updating timing; an updating
key holding unit for generating or holding in advance said
updating key; a data encryption unit for encrypting said
data using a data encryption key that is valid currently; a
25 data transmission unit for transmitting said data encrypted
by said data encryption unit to clients belonging to a
prescribed multicast group by multicasting; a key

encryption unit for encrypting the updating key
corresponding to the data encryption key that is valid
after the updating timing, at intervals of said updating
timing, using the data encryption key that is valid after
5 the updating timing; and an updating key transmission unit
for transmitting the updating key encrypted by said key
encryption unit to said at least one of clients by
unicasting or multicasting at intervals of said updating
timing.

10 According to the second aspect of the present
invention, the multicast server (or multicasting data
transmission device) transmits the data to clients
belonging to the multicast group by multicasting, after
encrypting it using the currently valid data encryption key.
15 The client receives the encrypted data transmitted from the
multicast server and decrypts this encrypted data using the
currently valid decryption key, which is the same as the
currently valid data encryption key. The multicast server
updates the data encryption key to a data encryption key
20 that is valid after the updating timing and is in a
relationship obtained by applying the updating key
corresponding to the data encryption key valid before this
updating timing to the data encryption key valid before
this updating timing, at intervals of a prescribed updating
25 timing. At intervals of the updating timing, the multicast
server transmits the updating key corresponding to the data
encryption key that is valid after the updating timing to

the client by unicasting or multicasting, encrypting it using the data encryption key that is valid after this updating timing. The client receives the encrypted updating key transmitted from the multicast server and
5 decrypts this encrypted updating key using the currently valid data decryption key. The client, on subscription to the data distribution service, updates the data decryption key that was valid before the updating timing to a data decryption key valid after the updating timing at intervals
10 of the updating timing, by generating a data decryption key valid after the updating timing applied from outside and subsequently by applying the updating key obtained by decryption performed using the data decryption key valid before this updating timing to the data decryption key
15 valid before this updating timing at intervals of the updating timing.

The same actions and effects as in the case of the first aspect described above can also be obtained with the second aspect of the present invention.

20

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a block diagram illustrating the overall layout of a multicast communication system according to a
25 first embodiment of the present invention;

Fig. 2 is a block diagram illustrating the construction of server 2;

Fig. 3 shows a data structure of a subscriber list;

Fig. 4 is a block diagram illustrating the layout of a distribution data receiving device (or adaptor);

Fig. 5 is a sequence diagram showing the flow of
5 processing of a server and a client belonging to a multicast group;

Fig. 6 is a block diagram illustrating the overall layout of a multicast communication system according to a second embodiment of the present invention;

10 Fig. 7 is a block diagram illustrating the layout of a server according to the second embodiment;

Fig. 8 shows key data whereby a plurality of group session keys Kgr and the key updating key Ku corresponding to each group session key Kgr are associated;

15 Fig. 9 is a block diagram illustrating the respective layouts of clients according to a second embodiment; and

Fig. 10 is a sequence diagram of illustrating the flow of processing of a server and a client belonging to the multicast group.

20

DESCRIPTION OF THE PREFERRED EMBODIMENTS

Embodiments of the present invention are described below with reference to the drawings. However, these are only examples and the technical scope of the present
25 invention is not restricted to these.

FIRST EMBODIMENT

Fig. 1 is a block diagram illustrating the overall layout of a multicast communication system according to a first embodiment of the present invention. This multicast communication system has a multicast server 2 connected to Internet 1, and a multicast group 3 having a plurality of clients 3a to 3d connected to Internet 1.

10 Multicast server (hereinafter simply called "server") 2 is a server that performs a data distribution service; it holds distribution data (content) such as music, video or text, and distributes this content through the Internet 1 to clients 3a to 3d belonging to multicast group 3 by IP multicasting.

15 Clients 3a to 3d belong to multicast group 3 and receive distributed data transmitted by IP multicasting from server 2. In Fig. 1, the number of clients was taken as four by way of example, but could be a number other than four.

20 In this multicast communication system, it is arranged that, of the clients 3a to 3d belonging to the multicast group 3, only clients (subscribers) that have subscribed to the data distribution service of server 2 by means of a prescribed subscription procedure (to be described later) can receive this data distribution service. This is implemented by server 2 transmitting the distribution data in encrypted form, clients belong to multicast group 3 becoming subscribers of the data distribution service by going through a prescribed subscription procedure and

acquiring a decryption key (this is a common key,
hereinafter referred to as "group session key Kgr") for
decrypting the encrypted distribution data.

That is, although all the clients of clients 3a to 3d
5 can receive distribution data relating to the data
distribution service from server 2 since they belong to
multicast group 3, it is arranged that, unless they have
become subscribers by going through a prescribed
subscription procedure, they cannot view/listen to the
10 distributed data by decrypting this received distributed
data.

Also, in this multicast communication system,
quantity-based charging is levied on the subscribers to the
data distribution service. In this embodiment, this
15 quantity-based charging is effected in accordance with time
after subscribing to the data distribution service.

Server 2, clients 3a to 3d and the details of the
processing which they perform are described below.

Fig. 2 is a block diagram illustrating the
20 construction of server 2. Server 2 has a control unit 20,
data encryption unit 21, key encryption unit 22,
transmission/reception unit 23, content database 24 and
subscriber list database 25.

Control unit 20 controls data encryption unit 21, key
25 encryption unit 22, transmission/reception unit 23, content
database 24 and subscriber list database 25 and performs
processing such as processing of subscription and

withdrawal of subscribers, as will be described in detail below, distribution of group session key Kgr on subscription, and quantity-based charging. Also, control unit 20 holds group session key Kgr and supplies group session key Kgr to this data encryption unit 21 and key encryption unit 22 on execution of encryption processing by data encryption unit 21 and key encryption unit 22.

Content database 24 is constituted by a storage device such as a hard disk or semiconductor memory or a recording medium such as a DVD or CD and reading device therefor and stores distribution data (content) transmitted to multicast group 3. This content database 24 supplies distribution data to data encryption unit 21 under the control of control unit 20.

Data encryption unit 21 receives the group session key (common key) Kgr from control unit 20 and, under the control of control unit 20, supplies distribution data from content database 24 to transmission/reception unit 23, encrypted using group session key Kgr. DES (data encryption standard) or the like is employed as the method of encryption. The group session key Kgr may be held by data encryption unit 21.

Subscriber list database 25 is constituted by a storage device such as a hard disk or semiconductor memory or a recording medium such as a DVD or CD and reading/writing device therefor and stores a subscriber list as shown in Fig. 3. The subscriber list is a list of

clients, of clients 3a to 3d belonging to the multicast group 3, which have subscribed to the data distribution list of server 2 through the prescribed subscription procedure. The subscribers registered in this subscriber list are supplied with group session key K_{gr} from server 2 and can thereby decrypt the encrypted distribution data from server 2.

As shown in Fig. 3, each list cell of the subscriber list includes the subscriber name, key decryption key K_m and date and time of subscription.

The "user name" is a name or identifier etc for uniquely identifying a given client from other clients; for example a unique user ID supplied to the subscriber by the provider of the data distribution service or the client's IP address etc could be employed as this user name.

The "key decryption key" is a common key for encrypting the group session key K_{gr} and for decrypting the encrypted group session key K_{gr} (hereinafter referred to as the "encrypted group session key K_{grx} "). This key decryption key is also possessed by the subscriber. Preferably the subscribers are provided with respective individual decryption keys $K_m(A)$, $K_m(B)$ etc.

The "subscription date and time" are the date and time at which the subscriber subscribed to the data distribution service. In this embodiment, the fees to be collected from the subscribers (data distribution service fees) are

calculated based on the time from the date and time of subscription to the date and time of withdrawal.

When a client belonging to multicast group 3 newly subscribes to the data distribution service, control unit 20 generates a new list cell and adds the generated list cell to the subscriber list. Conversely, when a client that is already subscribed withdraws from the data distribution list, control unit 20 deletes the list cell of the withdrawn subscriber from the subscriber list.

10 Key encryption unit 22 receives the group session key Kgr from control unit 20, reads the key decryption key Km of the transmission-end client from the subscriber list under the control of control unit 20, and encrypts the group session key Kgr using the key decryption key Km which
15 has thus been read. As the method of encryption, DES (data encryption standard) or the like is employed. Key encryption unit 22 then supplies the encrypted group session key Kgrx that has been obtained by the encryption process to transmitting/reception unit 23. For example, if
20 the group session key Kgr is transmitted to client 3a, key encryption unit 22 encrypts the group session key Kgr using key decryption key Km(A) of client 3a.

Transmitting/reception unit 23 constitutes an interface device with Internet 1. This
25 transmitting/reception unit 23 sends data from data encryption unit 21 to clients belonging to multicast group 3 under the control of control unit 20 by IP multicasting

through Internet 1 and sends the encrypted group session
keys K_{grx} from key encryption unit 22 to the clients by
unicasting through Internet 1. Also,
transmitting/reception unit 23 receives data sent from the
5 clients belonging to the multicasting group 3 through
Internet 1 and supplies this to control unit 20.

A distributed data receiving device (or adaptor) is
mounted in clients 3a to 3d; this constitutes a hardware
device for receiving distributed data from server 2. This
10 distributed data receiving device is put in a condition
whereby it can be purchased by any user by for example
being sold on the market and is purchased in order to
enable users of clients 3a to 3d to subscribe to the data
distribution service. A key decryption key K_m for
15 decrypting an encrypted group session key K_{grx} is stored
beforehand in this distribution data receiving device.

Fig. 4 is a block diagram illustrating the layout of a
distribution data receiving device (or adaptor) 300. This
distributed data receiving device 300 has a control unit 30,
20 transmitting/reception unit 31, data decryption unit 32,
key decryption unit 33 and key decryption key holding unit
34.

Control unit 30 controls transmitting/reception unit
31, data decryption unit 32, key decryption unit 33, and
25 key decryption key holding unit 34 and, as will be
described in detail later, also performs processing such as
processing for entry and withdrawal of a subscriber and

deletion (or destruction) of group session key K_{gr} and
deletion (or destruction) of key decryption key K_m on
withdrawal.

Transmitting/reception unit 31 is an interface device
5 with Internet 1 and transmits a reception request (to be
described later) supplied from control unit 30 under the
control of control unit 30 to server 2 through Internet 1.
Also, transmitting/reception unit 31, under the control of
control unit 30, receives incoming encrypted group session
10 key K_{grx} and encrypted distributed data (hereinbelow
referred to as "encrypted distribution data") sent from
server 2 through Internet 1 and respectively supplies these
to key decryption unit 33 and data decryption unit 32.

Key decryption key holding unit 34 holds key
15 decryption key K_m . Key decryption key K_m is preferably
stored (formed) in key decryption key holding unit 34 in
the form of a hardware circuit (for example an IC chip) to
ensure that key decryption key K_m cannot easily be read by
a third party (third person, other people). Also,
20 preferably, different key decryption keys K_m are stored in
each distribution data receiving device (i.e. client).

Key decryption unit 33 uses the key decryption key K_m
to decrypt the encrypted group session key K_{grx} sent from
server 2 and holds the group session key K_{gr} obtained by
25 this decryption. It would be possible for data decryption
unit 32 to hold group session key K_{gr} .

1002409 16304
Data decryption unit 32 decrypts the encrypted
distribution data sent from server 2 using the group
session key K_{gr} that is held by key decryption unit 33 and
supplies the distribution data obtained by decryption to a
5 client where distribution data receiving device 300 is
mounted. The client outputs the distribution data to its
display device (CRT display, liquid crystal display etc)
and to its speakers etc. The user of the client can
thereby view/listen to etc the distributed data. The
10 distributed data may be stored in a storage device (not
shown) such as the client's hard disk, before being output.

As will be described, the key decryption key K_m that
is stored in key decryption key holding unit 34 and the
group session key K_{gr} that is held by key decryption unit
15 33 are deleted (or destroyed) by control unit 30 in
response to withdrawal of the client from the data
distribution service.

Fig. 5 is a sequence diagram showing the flow of
processing of server 2 and a client (in this case, this
20 will be assumed to be client 3c) belonging to multicast
group 3. The processing shown in this sequence diagram
describes the case where a client 3c that has not yet
subscribed to the data distribution service of server 2
subscribes to this data distribution service.

25 At first, since client 3c is not subscribed to the
data distribution service, it is in the condition that

although encrypted distribution data sent by server 2 can be received, this cannot be decrypted.

In this condition, first of all, the user of client 3c purchases a distribution data receiving device 300 and
5 mounts this in client 3c. It is to be assumed that key decryption key $Km(C)$ is stored in distribution data receiving device 300 mounted in client 3c.

In response to mounting distribution data receiving device 300 in client 3c, as the data subscription service
10 subscription procedure, control unit 30 transmits a reception request to server 2 (step S1) through transmitting/reception unit 31 and Internet 1. This reception request includes the client name of client 3c and an equipment number (identification number/serial number)
15 for uniquely identifying distribution data receiving device 300 mounted in client 3c from other distribution data receiving devices.

This equipment number may be stored beforehand in control unit 30 and transmitted by control unit 30, or a
20 number pasted onto the substrate etc of distribution data receiving device 300 may be input from client 3c by the user of client 3c and transmitted by control unit 30. Also, server 2 is informed of this equipment number from the sales point immediately after purchase of distribution data
25 receiving device 3 and stores it in control unit 20.

The reception request transmitted through the Internet 1 from client 3c is supplied to control unit 20 through

transmitting/reception unit 23 (see Fig. 2) of server 2.
Control unit 20 determines whether or not to allow
reception (step S21) by ascertaining whether or not the
equipment number contained in the reception request is that
5 of which was informed from the sales point.

If the equipment number contained in the reception
request is the same as that of which was informed from the
sales point, control unit 20 allows reception (step S21:
YES); otherwise, it does not allow reception (step S21: NO).

10 If reception is not allowed, control unit 20 ignores
the reception request (step S33). The condition that
client 3c is unable to view/listen to distribution data
therefore continues.

If reception is allowed, control unit 20 generates a
15 list cell of the subscriber list and adds this list cell
that has been generated to the subscriber list of
subscriber list database 25 (step S23). The client's name
included in the reception request is stored in the client's
name column of this list cell and the key decryption key
20 ("Km(C)") stored in key decryption key holding unit 34 of
distribution data receiving device 300 is stored in the key
decryption key column. Also, as the subscription date and
time, the date and time of the reception request (or the
date and time of generation of the list cell or the date
25 and time of registration in database 25 etc) are stored.

If the key decryption keys Km are different for each
distribution data receiving device 300, equipment

number/key decryption key association data associating the
equipment numbers of distribution data receiving devices
300 and the key decryption keys K_m stored in their key
decryption key holding units 34 is stored beforehand in
5 server 2 (for example control unit 20 or a storage unit,
not shown). The key decryption key K_m associated with the
equipment number is thereby stored under the "key
decryption key" of the list cell by control unit 20.

Next, key encryption unit 22 encrypts the group
10 session key K_{gr} to encrypted group session key K_{grx} using
key decryption key $K_m(C)$, and sends the encrypted group
session key K_{grx} through transmitting/reception unit 23 to
client 3c by multicasting (step S25).

When the transmitting/reception unit 31 of
15 distribution data receiving device 300 receives the
encrypted group session key K_{grx} , it supplies the encrypted
group session key K_{grx} that has thus been received to key
decryption unit 33. Key decryption unit 33 decrypts the
encrypted group session key K_{grx} using the key decryption
20 key $K_m(C)$ held by key decryption key holding unit 34 and
holds this decrypted group session key K_{gr} (step S5). The
subscription procedure is thereby completed.

After this, data encryption unit 21 of server 2
encrypts the distribution data stored in content database
25 24, using group session key K_{gr} , and sends this to the
multicast group 3 by IP multicasting through
transmitting/reception unit 23 (step S27).

When transmitting/reception unit 31 of client 3c receives the encrypted distribution data, it supplies this encrypted distribution data to data decryption unit 32. Data decryption unit 32 decrypts the encrypted distribution data using the group session key Kgr held by key decryption unit 33, and supplies the decrypted distribution data to client 3c. If the distribution data contains video data, client 3c displays this video data on a display device; if it contains voice data, it outputs this voice from the speakers (step S7).

This processing of steps S5 and S7 is repeated until client 3c withdraws from the data distribution service (step S9: NO).

However, when client 3c does withdraw from the data distribution service (step S9: YES), the withdrawal request from client 3c is supplied to control unit 30. This withdrawal request is for example input by the user of client 3c by means of an input device (keyboard etc) of client 3c.

When control unit 30 receives a withdrawal request from client 3c, it deletes (or destroys) the key decryption key Km(C) held in key decryption key holding unit 34 and deletes (or destroys) the group session key Kgr held in key decryption unit 33. Also, with this deletion, control unit 30 generates a deletion value as data indicating that deletion has taken place (step S11).

Control unit 20 of server 2 determines (step S29) whether the deletion value is legitimate or not. This determination is performed by control unit 20 performing the same calculation as control unit 30 and comparing the
5 result of this calculation with the received deletion value. If for example, as the deletion value, the result of performing a prescribed calculation on the equipment number is employed, control unit 20 performs the same calculation as control unit 30 on the equipment number of distribution
10 data receiving device 300 (client 3c) that transmitted the deletion value and ascertains whether the deletion value is legitimate or not by comparing this calculated result with this deletion value.

Also, where the result of the performing a prescribed
15 calculation on an index number or the result of performing a prescribed calculation on the data and time of termination of reception is employed as the deletion value, the determination may be made by performing a reverse calculation on the deletion value and ascertaining whether
20 the result of the reverse calculation is appropriate or not. Since in this case it is possible to ascertain from the result of the reverse calculation (index number or date and time of termination of reception) to what point of the data stream reception by client 3c has been achieved or to
25 ascertain the date and time of termination of reception, this can be used to perform quantity-based charging.

If the deletion value is legitimate (step S29: YES), control unit 20 finds the time of subscription to the service from the date and time of subscription of the list cell of client 3c and the data and time at which the deletion value was received, and calculates a quantity-based service fee in accordance with this time. This service fee is then charged to or collected from the user of client 3c. Charging and collection may be performed during the subscription period at fixed periods (for example of one month) and, on withdrawal, charging may be effected in accordance with the period from the time point at which charges were last levied prior to withdrawal up to the time point of withdrawal. Also, if the index value or the date and time of termination of reception is obtained from the deletion value, quantity-based charging may be effected using this index value or the date and time of termination of reception.

After this, control unit 20 deletes the list cell of client 3c from the subscriber list of subscriber list database 25. The result of this deletion is that service charges are no longer applied to client 3c.

If, on the other hand, the deletion value is not legitimate (step S29: NO), control unit 20 deems client 3c to be an offender and sends a warning to client 3c (step S35).

Thus, in this embodiment, in IP multicast communication, the distribution data is encrypted and only

parties who have properly subscribed to the data
distribution service can acquire the decryption key.
Consequently, in IP multicasting, encryption is
appropriately performed and, as a result, only parties that
5 have properly subscribed to the data distribution service
can view/listen to the distribution data, while secrecy of
the data is guaranteed against other parties. Also, in
this embodiment, management/control of subscribers to the
data distribution service can be performed at server 2 that
10 is the source of provision of the distribution data.
Furthermore, with this embodiment, more finely graduated
quantity-based charges can be applied than in the case of
charging using the pay-per-view system.

It should be noted that, instead of obtaining the key
15 decryption keys K_m of the clients (distribution data
receiving devices 300) of server 2 from the equipment
number/key decryption key association data as described
above, it would be possible for the distribution data
receiving devices 300 to send their own key decryption keys
20 K_m to server 2 in a form encrypted using a public key K_p of
server 2 and for server 2 to obtain these transmitted keys
by decrypting them using secret key K_s . In this case, the
need for equipment number/key decryption key association
data to be provided in server 2 is eliminated. As a public
25 key encryption system using such a public key and secret
key, RSA (Rivest Shamir Adleman) or elliptical curve
encryption etc may be employed.

Also, PKI (public key infrastructure) may be employed. Specifically, when each client subscribes to the data distribution service, it receives a digital certificate (set of public key and secret key) issued by the authorization office of the PKI. Thus, when server 2 receives a reception request from a client, it acquires the public key (client's public key) of this digital certificate and encrypts the group session key Kgr using this public key; the client that sent the reception request then decrypts the encrypted group session key Kgrx obtained by this encryption process using the secret key of the digital certificate and can thereby acquire the group session key Kgr.

SECOND EMBODIMENT

Secrecy of the distribution data can be ensured by periodically updating the group session key Kgr.

Fig. 6 is a block diagram illustrating the overall layout of a multicast communication system according to a second embodiment of the present invention. This multicast communication system has a multicast server 4 connected to the Internet 1 and a multicast group 5 having a plurality of clients 5a to 5d connected to the Internet 1. The overall layout of this multicast communication system is the same as in the case of the first embodiment illustrated in Fig. 1, so a description of the overall layout of this multicast communication system will here be omitted.

Fig. 7 is a block diagram illustrating the layout of server 4 according to the second embodiment. Server 4 has a control unit 40, data encryption unit 41, key encryption unit 42, transmitting/reception unit 43, content database 44, subscriber list database 45 and key database 46.

Control unit 40 controls data encryption unit 41, key encryption unit 42, transmitting/reception unit 43, content database 44, key database 45 and subscriber list database 46 and performs processing such as processing for subscription and withdrawal of subscribers, as will be described in detail later, distribution of group session key Kgr on subscription, and quantity-based charging etc. Also, control unit 40 updates the group session key Kgr at intervals of a fixed time T1.

Content database 44 is similar to the content database 24 (see Fig. 2) in the first embodiment. The distribution data stored in this content database 44 is read and supplied to data encryption unit 41 under the control of control unit 40.

Data encryption unit 41 receives the group session key (common key) Kgr from control unit 40 and, under the control of control unit 40, encrypts the distribution data from content database 44 using group session key Kgr before supplying it to transmitting/reception unit 43. As the method of encryption, DES or the like may be employed. The group session key Kgr may be held by data encryption unit 41.

Subscriber list database 46 is constructed in the same way as subscriber list database 25 (see Fig. 2) in the first embodiment and stores a list of subscribers who have subscribed to the data distribution service through a prescribed subscription procedure. This subscriber list is practically the same as that of the first embodiment illustrated in Fig. 3, but, in this embodiment, the column "key decryption key Km" that is found in the first embodiment is not provided.

As shown in Fig. 8, the key database 45 holds key data whereby a plurality of group session keys Kgr and the key updating key Ku corresponding to each group session key Kgr are associated.

If symbol i is an arbitrary positive value, group session key $Kgr(i+1)$ is obtained by applying the key updating key $Ku(i)$ corresponding thereto to the group session key $Kgr(i)$. An example of a process whereby this action may be performed is a process of calculation by substituting the group session key $Kgr(i)$ and the key updating key $Ku(i)$ in a prescribed equation (including processing whereby the group session key $Kgr(i)$ is encrypted using key updating key $Ku(i)$). Group session key $Kgr(1)$ is supplied beforehand to key database 45 as the initial value of the group session key.

The arrangement is such that, of the group of this plurality of group session keys Kgr, data encrypted using an arbitrary group session key $Kgr(i)$ can only be decrypted

using the same group session key $K_{gr}(i)$ and cannot be decrypted using another group session key $K_{gr}(j)$ ($i \neq j$).

Control unit 40 updates group session key K_{gr} from $K_{gr}(i)$ to $K_{gr}(i+1)$ at intervals of a fixed time T_1 .

- 5 Control unit 40 then, on this updating (with the updating timing) encrypts the key updating key $K_u(i)$ using group session key $K_{gr}(i)$, and sends the encrypted key updating key to the clients belonging to multicast group 5.

- As the key updating keys $K_u(i)$, new keys may be
- 10 successively generated by control unit 40, or only a prescribed number n of keys may be prepared beforehand. In the former case, pseudo-random numbers or the like generated by for example a pseudo-random number generator may be employed as the new key updating keys. In the
- 15 latter case, a cyclic arrangement is produced whereby the first group session key $K_{gr}(1)$ is generated when the n -th group session key $K_{gr}(n)$ acts on the key updating key $K_u(n)$.

- Also, it is not necessarily essential for a plurality of group session keys to be stored in key database 45: it
- 20 would be possible to store only the currently active group session key K_{gr} (i.e. the group session key K_{gr} that is currently being employed for encryption of the distribution data). In this case, control unit 40 creates the next
- group session key $K_{gr}(i+1)$ by applying the key updating key
- 25 $K_u(i)$ corresponding thereto to the currently active group session key $K_{gr}(i)$ on the key updating.

Key encryption unit 42 receives the group session key $K_{gr}(i)$ from control unit 40. Then, on updating of the group session key of control unit 40, key encryption unit 42 reads the key updating key $K_u(i)$ corresponding to the group session key $K_{gr}(i)$ from key database 45 and encrypts this using group session key $K_{gr}(i)$ and supplies the encrypted key updating key $K_u(i)$ (hereinbelow called "encrypted key updating key $K_{ux}(i)$ ") to transmitting/reception unit 43. This encrypted key updating key $K_{ux}(i)$ is sent to the clients belonging to multicast group 5 from transmitting/reception unit 43 through Internet 1. DES or the like may be employed as the method of encryption.

Transmitting/reception unit 43 is an interface device with Internet 1 and sends the data from data encryption unit 41 or key encryption unit 42 to the clients belonging to the multicast group 5 through Internet 1 under the control of control unit 20 and receives incoming data sent through Internet 1 from the clients belonging to multicast group 5 and supplies this to control unit 40.

Fig. 9 is a block diagram illustrating the respective layouts of clients 5a to 5d according to a second embodiment. Since all the clients 5a to 5d have the same layout, only that of client 5c is described below as a typical example.

Client 5c has control unit 50, transmitting/reception unit 51, data decryption unit 52, key decryption unit 53, output unit 54, input unit 55 and key generating unit 56.

Control unit 50 controls transmitting/reception unit 51, data decryption unit 52, key decryption unit 53, output unit 54 and input unit 55 and performs processing such as processing of subscription and withdrawal of a subscriber, as will be described in detail later, and deletion (destruction) of group session key $K_{gr}(i)$ on withdrawal.

Transmitting/reception unit 51 is an interface device with Internet 1 and transmits a reception request (to be described later) supplied from control unit 50 to server 4 through Internet 1 under the control of control unit 50. Also, transmitting/reception unit 51, under the control of control unit 50, receives incoming encrypted distribution data and encrypted key updating key $K_{ux}(i)$ transmitted from server 4 through Internet 1 and supplies these respectively to data decryption unit 52 and key decryption unit 53.

Key decryption unit 53 decrypts the encrypted key updating key $K_{ux}(i)$ transmitted from server 4 using group session key $K_{gr}(i)$ and holds the key updating key $K_u(i)$ obtained by this decryption. The key updating key $K_u(i)$ obtained by decryption may be supplied to key generating unit 56 and held.

Key generating unit 56 receives key updating key $K_u(i)$ held by key decryption unit 53 and generates the next group session key $K_{gr}(i+1)$ from this and key updating key $K_u(i)$

and the group session key $K_{gr}(i)$ corresponding to this.
Also, key generating unit 56 holds the currently active
group session key $K_{gr}(i)$ and the group session key $K_{gr}(i+1)$
which will next become active.

5 Data decryption unit 52 decrypts the encrypted
distribution data transmitted from server 4 using the
currently active group session key $K_{gr}(i)$ that is held by
key generating unit 56 and supplies the decrypted
distribution data to output unit 54.

10 Output unit 54 is constituted of a display device (CRT
display/liquid crystal display or the like) and/or speakers
etc and outputs the distribution data supplied from data
decryption unit 52. The user of client 5c can thereby
view/listen to etc the distribution data. The distribution
15 data could also be stored in a storage device (not shown)
such as a hard disk of client 5c before being output by
output unit 54.

As will be described later, the group session keys
 $K_{gr}(i)$ and $K_{gr}(i+1)$ stored in key generating unit 56 are
20 deleted (or destroyed) by control unit 50 in response to
withdrawal of client 5c from the data distribution service.

Fig. 10 is a sequence diagram of illustrating the flow
of processing of server 4 and a client belonging to the
multicast group 5 (in this case assumed to be client 5c).
25 The processing shown in this sequence diagram describes the
case where a client 5c which has not yet subscribed to the

data distribution service of server 4 subscribes to this data distribution service.

First of all, the control unit 50 of client 5c performs the subscription procedure of the data distribution service in accordance with user instructions supplied through input unit 55 of client 5c. This subscription procedure is performed by control unit 50 transmitting a reception request to server 4 through transmitting/reception unit 51 and Internet 1 (step S51). This transmission request includes the client name of client 5c.

The reception request is supplied to control unit 40 through transmitting/reception unit 43 of server 4. Control unit 40 determines whether or not to allow reception (step S81) by ascertaining whether the client name included in the reception request is that of a client belonging to the multicast group 5 and whether this client is not subscribed to the data distribution service.

Control unit 40 permits reception (step S81: YES) for clients belonging to the multicast group 5 whose client name is contained in the reception request and which were not subscribed to the data distribution service; otherwise it does not permit reception (step S81: NO).

If reception is not permitted, control unit 40 ignores the reception request (step S85). The condition that client 5c cannot view/listen to the distributed data therefore continues.

If reception is permitted, control unit 40 generates a list cell of the subscription list for client 5c and adds this list cell that has been generated to the subscriber list of subscriber list database 46 (step S83). In the "client name" column of this list cell, the client name included in the reception request is stored; in the "date and time of subscription" the date and time of reception of the reception request (or the date and time of generation of the list cell/date and time of registration on database 46 etc) is stored.

Next, control unit 40 (or key encryption unit 42) encrypts the group session key (let this be $K_{gr}(i)$) that is active at the time point of reception of the reception request and transmits this (step S87) by unicasting to client 5c through transmitting/reception unit 43. Example methods for this encryption include encrypting the group session key $K_{gr}(i)$ by server 4 with common key K_c and encrypting this common key K_c using the public key K_p of client 5c before transmitting the encrypted $K_{gr}(i)$ (i.e., $K_{grx}(i)$) and encrypted K_c to client 5c. Client 5c uses secret key K_s to decrypt the encrypted common key K_c and further decrypts the encrypted group session key $K_{grx}(i)$ using common key K_c , to obtain the group session key $K_{gr}(i)$ (step S53).

Next, key encryption unit 42 uses the group session key $K_{gr}(i)$ to encrypt the key updating key $K_u(i)$, thereby generating an encrypted key updating key $K_{ux}(i)$, and

transmits this encrypted key updating key $K_{ux}(i)$ to client 5c by unicasting (step S89).

Next, data encryption unit 41 encrypts the distribution data stored in content database 44 using group session key $K_{gr}(i)$ and transmits this encrypted distribution data to the multicast group 5 by multicasting (step S91). If the transmission time (step S89) of unicasting of the encrypted key updating key $K_{ux}(i)$ corresponds to the key updating time (updating timing) of another client (other clients), transmission of this encrypted key updating key $K_{ux}(i)$ to multicast group 5 may be effected by multicasting rather than transmission solely to client 5c by unicasting.

The key decryption unit 53 of client 5c decrypts the encrypted key updating key $K_{ux}(i)$ using group session key $K_{gr}(i)$ and holds the decrypted key updating key $K_u(i)$ (step S55). Next, key generating unit 56 generates the next group session key $K_{gr}(i+1)$ by applying the key decryption key $K_u(i)$ held in key decryption unit 53 to group session key $K_{gr}(i)$ and holds this (step S57).

Data decryption unit 52 uses the group session key $K_{gr}(i)$ to decrypt the encrypted distribution data and supplies the distribution data obtained by this decryption to output unit 54 (step S59). Output unit 54 outputs the distribution data and thereby enables the user of client 5c to view/listen to the distribution data (step S61).

The distribution data is encrypted and transmitted (step S93: NO, S91) using this group session key $K_{gr}(i)$ in server 4 until the key updating timing arrives, at intervals of time $T1$.

5 When the key updating timing arrives (step S93: YES), control unit 40 updates (step S95) the group session key $K_{gr}(i)$ to the next group session key $K_{gr}(i+1)$.

Next, key encryption unit 42 encrypts the key updating key $Ku(i+1)$ corresponding to group session key $K_{gr}(i+1)$ using group session key $K_{gr}(i+1)$ and transmits the encrypted key updating key $Kux(i+1)$ obtained by this encryption to the multicast group 5 by multicasting (step S97).

When transmitting/reception unit 51 of client 5c receives this encrypted key updating key $Kux(i+1)$, control unit 50 instructs key generating unit 56 to update the group session key $K_{gr}(i)$ to the next group session key $K_{gr}(i+1)$. Subsequently, data decryption unit 52 uses group session key $K_{gr}(i+1)$ to decrypt the encrypted distribution data. The group session key $K_{gr}(i)$ and key updating key $Ku(i)$ that were used immediately previously are deleted (or destroyed) by control unit 50.

Also, simultaneously with this, key decryption unit 53 uses the group session key $K_{gr}(i+1)$ to decrypt the encrypted key updating key $Kux(i+1)$. Key generating unit 56 generates and holds the next group session key $K_{gr}(i+2)$

by applying this key updating key $Ku(i+1)$ obtained by decryption to the group session key $Kgr(i+1)$.

The same processing is performed in respect of other clients belonging to multicast group 5 and that have
5 subscribed to the data distribution service.

This updating of the group session key is repeated at intervals of time $T1$. In this way, it is made difficult for a third party who is not subscribed to the data distribution service to decrypt the distribution data so as
10 to view/listen to it, thereby guaranteeing high secrecy of the distribution data.

In contrast, when client 5c withdraws from the data distribution service, in the same way as the first embodiment described above, control unit 50 deletes
15 (destroys) (not shown in Fig. 10) all of the concurrently active group session key and next group session key and key updating key stored in key generating unit 56. Thus, client 5c is thereafter unable to decrypt encrypted distribution data and is also unable to update subsequent
20 group session keys. As a result, the user of client 5c cannot view/listen to distribution data after withdrawal.

Control unit 50 then sends (not shown in Fig. 10) the deletion value and the client name to server 4. As the deletion value, the result of performing prescribed
25 calculation (calculation using a prescribed equation, hash calculation etc) on identification information of client 5c (for example its IP address) can be employed or, in the

same way as in the first embodiment, the result of performing a prescribed calculation on the index number or the result of performing a prescribed calculation on the date and time of transmission of the withdrawal request etc
5 could be employed.

Server 4 ascertains whether the deletion value is legitimate or not and, if it is legitimate, deletes (not shown in Fig. 10) the list cell of client 5c that sent the deletion value from the subscriber list of subscriber data
10 base 46. If the deletion value is not legitimate, server 4 issues a warning (not shown in Fig. 10) to the client 5c that transmitted the deletion value. In this way, server 4 is able to accurately identify subscribers that have subscribed to the data distribution service and can perform
15 charging for the data distribution service appropriately. The method of charging can be the same as in the case of the first embodiment described above.

It should be noted that, if the transmissions shown in step S87 and S89 shown in Fig. 10 are both performed by
20 unicasting, transmission could be performed simultaneously by a single transmission of the encrypted group session key Kgrx and encrypted key updating key Kux. Also, in step S53 and/or step S55, if reception by client 3c is unsuccessful, server 4 can be made to retransmit by sending a
25 retransmission request to server 4.

Also, at fixed time intervals $T2 (T1)$, the currently active group session key can be converted to another group

session key not in a correlated relationship with this group session key by performing unicast communication between server 4 and the clients subscribed to the data distribution service. In this way, even if a client that was not subscribed to the data distribution service has illegally acquired encrypted key K_{gr} , this client can be prevented from decrypting data relating to the data distribution service.

10 OTHER EMBODIMENTS

The Internet 1 in the first and second embodiments could be an intranet.

Also, the content database 24 (44) and subscriber list database 25 (46) in the first and second embodiments, instead of being on the same server, could be respectively held and managed on separate servers. In this case, a client belonging to multicast group 3 (5) performs registration of subscription to the data distribution service with the server (subscriber management server) that holds the subscriber list database 25 (46) and receives data relating to the data distribution service from a server (data server) that holds the content database 24 (44). It can be arranged for a client that is subscribed to the server to receive the group session key and key updating key etc from the subscriber management server or to receive these from the data server. Likewise, charging

of the service fee may be conducted by the subscriber management server or may be conducted by the data server.

The processing of the server 2 and distribution data receiving device 300 in the first embodiment may be realized by hardware circuitry or may be realized by a program and a CPU or microcomputer that executes this program. Preferably, however, as described above, the key decryption key Km of distribution data receiving device 300 is formed by a hardware circuit or IC chip.

Likewise, the processing of server 4 and client 5 in the second embodiment may be realized by hardware circuitry or may be realized by a program and a CPU or microcomputer that executes this program.

According to the present invention, in multicast communication, data encryption can be appropriately performed. Also, according to the present invention, the multicast server or the server that manages the subscribers to the data distribution service can ascertain and control which clients, of the clients belonging to the multicast group, are subscribed to the data distribution service. Furthermore, according to the present invention, charging can be performed in accordance with the amount of data received from subscription to withdrawal or quantity-based charging with fine gradations can be performed by performing charging in accordance with the time from subscription to withdrawal.